

# Oppfølging av forvaltningsrevisjon IKT-sikkerhet

---

**Behandles i utvalg**

Kontrollutvalget i Rennebu kommune

**Møtedato**

21.02.2024

**Saknr**

05/24

**Saksbehandler** Ragnhild Aashaug

**Arkivkode** FE-217, TI-&58

**Arkivsaknr** 23/224 - 8

---

**Forslag til vedtak**

Kontrollutvalget tar informasjonen til orientering.

**Vedlegg**

Tilbakemelding oppfølging IKT-sikkerhet Rennebu kommune - rapport forvaltningsrevisjon  
Organisasjonkart IT-revisjon

**Saksopplysninger**

Kommunestyret behandlet i sak 28/2023 i møte den 22.06.2023 forvaltningsrevisjon "IKT-sikkerhet Rennebu kommune". Kommunestyret fattet dette vedtaket:

Forvaltningsrevisjonsrapporten IT-Sikkerhet av 25.05.23 tas til etterretning. Rennebu kommune følger revisors anbefalinger og kommunestyret ber kommunedirektøren sørge for å:

1. Iverksette et arbeid med identifisering av informasjonsverdier, vurdering av trusler og sårbarheter som grunnlag for spesifikke sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganiseringen. Dette arbeidet kan munne ut i en overordnet plan for IKT og IKT-sikkerhet.
2. Avklare og dokumentere organiseringen av informasjonssikkerhetsarbeidet og være konsekvent i benevnelsen av roller.
3. Vurdere å sikre at rutinen for tilgangsstyring etterleves ved endring og avslutning av arbeidsforhold, herunder også innlevering av kommunens datautstyr.
4. Vurdere behovet for dokumentasjon av IKT-hendelser som grunnlag for evaluering og læring.
5. Utarbeide en plan for hendelseshåndtering og gjenoppretting.

Kommunedirektøren rapporterer til kontrollutvalget om iverksatte tiltak innen 01.12.23.

Kommunedirektøren har sendt over et notat som viser hvordan oppfølgingen er gjort. Han vil også komme og redegjøre for saken i møtet.

**Status for anbefalingene**

Sekretariatet har gjort en kort oppsummering ut fra tilbakemelding for anbefalingene:

1. Iverksette et arbeid med identifisering av informasjonsverdier, vurdering av trusler og sårbarheter som grunnlag for spesifikke sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganiseringen. Dette arbeidet kan munne ut i en overordnet plan for IKT og IKT-sikkerhet.

Det fremgår at det flere dokumenter som beskrives rutine våre, og som er samlet i egen mappe med ulike beskrivelser for IKT- organisering og sikkerhet. Det er uklart for sekretariatet om dette er å betrakte som en overordnet plan for IKT og IKT-sikkerhet. Kontrollutvalget bør få klarhet i dette i møtet.

2. Avklare og dokumentere organiseringen av informasjonssikkerhetsarbeidet og være konsekvent i benevnelsen av roller.

Organisasjonskartet er revidert og viser tydelige roller – se vedlegget.

3. Vurdere å sikre at rutinen for tilgangsstyring etterleves ved endring og avslutning av arbeidsforhold, herunder også innlevering av kommunens datautstyr.

Det er etablert rutiner for tilgangsstyring, men at dette må jobbes mer med i hele organisasjonen. Det er planlagt for dette i 2024. Det samme gjelder innlevering av kommunens datautstyr.

4. Vurdere behovet for dokumentasjon av IKT-hendelser som grunnlag for evaluering og læring.  
Det er under utarbeidelse et årshjul som sikrer at faste rutiner blir ivaretatt.
5. Utarbeide en plan for hendelseshåndtering og gjenoppretting.  
Det er under planlegging en IT-øvelse i 2024 som vil være et godt utgangspunkt for å ytterligere forbedre våre interne rutiner ifm. hendelseshåndtering og gjenoppretting.  
Det er også varslet øvelse fra Stasforvalter våren 2024.

### **Saksvurdering og konklusjon**

Alle oppfølgingspunktene er beskrevet med rutineendringer - noe er gjort og noe er planlagt. Det essensielle er om oppfølgingen bidrar til å bedre kommunens tjenester, rutiner og verktøy. Kontrollutvalget skal ikke ha noen formening om hvordan oppfølgingen gjøres, men de skal ha et inntrykk av at de iverksatte tiltak bidrar til en forbedring. Dersom kontrollutvalget under orienteringen ikke finner at punktene overfor er tilstrekkelig oppfylt, kan kontrollutvalget be om en ytterligere oppfølging.